This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Please add claims 16 and 17.
Amend claims

1. (Currently Amended) A method for transferring ~~In a communication system having a a storage system for receiving~~ encrypted content via a ~~an IEEE 1394 serial~~ bus in a system where keys are periodically changed, ~~the storage system including storage media for storing content, a method for storing the encrypted content on the storage media,~~ the method comprising:

receiving the encrypted content via the ~~IEEE 1394~~ bus;

receiving a first ~~negotiated~~ key for decrypting the encrypted content;

encrypting the first ~~negotiated~~ key with ~~to form~~ a second key to form an encrypted first key;

combining the encrypted content with the ~~second~~ encrypted first key to form a combined encrypted content;

storing the combined encrypted content on [[the]] a storage media;

in response to a request for the stored encrypted content, decrypting the encrypted content to obtain clear text content;

encrypting the clear text content with a ~~negotiated transmission~~ third key; and

transmitting the encrypted content via the ~~IEEE 1394~~ bus.

2. (Currently Amended) The method of claim 1, wherein said decrypting step further comprising:

retrieving the combined encrypted content from the storage media;

decrypting the encrypted first key ~~second key~~ to obtain the first ~~negotiated~~ key; and

decrypting the encrypted content with the first ~~negotiated~~ key to recover clear text content.

3. (Currently Amended) The method of claim 1, further comprising:
further encrypting the <u>encrypted first</u> ~~second~~ key prior to storage on the single media.

4. (Currently Amended) The method of claim 1, wherein the <u>first key is a newly negotiated key</u> ~~combined encrypted content includes a stream~~.

5. (Currently Amended) The method of claim <u>1</u> [[4]], further comprising:
<u>storing the second key with the combined encrypted content on the storage media</u> ~~including a header in the combined encrypted content~~.

6. (Currently Amended) The method of claim <u>1</u> [[4]], ~~further comprising~~ <u>wherein the second key is stored in a header of a file that includes the combined encrypted content</u>
~~receiving the second key and the encrypted data;~~
~~decrypting the second key to form the first key; and~~
~~decrypting the encrypted data with the first key to form clear text.~~

7. (Canceled)

8. (Previously Presented) The method of claim 3, wherein the further encrypting uses a different algorithm than that used in encrypting the first key.

9. (Previously Presented) The method of claim 8, wherein an algorithm includes one or more of DES, XOR, M2, M6+, IDEA.

10. (Currently Amended) An apparatus for <u>transferring encrypted content via a bus in a system where keys are periodically changed, the method comprising:</u>
<u>a processor;</u>

a machine-readable medium including instructions executable by a processor for:

receiving the encrypted content via the bus;

receiving a first key for decrypting the encrypted content;

encrypting the first key with a second key to form an encrypted first key;

combining the encrypted content with the encrypted first key to form a combined encrypted content;

storing the combined encrypted content on a storage media;

in response to a request for the stored encrypted content, decrypting the encrypted content to obtain clear text content;

encrypting the clear text content with a third key; and

transmitting the encrypted content via the bus.

storing encrypted content on a storage media comprising:

~~an interface module for receiving encrypted content and a first negotiated key for decrypting the encrypted content over an IEEE 1394 bus, said interface module adapted to encrypt said first negotiated key to form a second key, and for combining the encrypted content with the second key to form a combined encrypted content; and~~

~~a storage media device for receiving and storing the combined encrypted content.~~

11. (Previously Presented) The apparatus of claim 10, wherein the combined encrypted content includes a stream.

12. (Currently Amended) The apparatus of claim 11, further comprising: ~~wherein said~~ an interface module ~~includes~~ including a combiner for combining a header with the combined encrypted content stream.

13. (Currently Amended) The apparatus of claim 10, wherein the encrypted first ~~second~~ key is further encrypted prior to storage on the storage media device.

14. (Previously Presented) The apparatus of claim 13, wherein the further encrypting uses a different algorithm than that used in encrypting the first key.

15. (Previously Presented) The apparatus of claim 14, wherein the algorithm used by said combiner includes one or more of DES, XOR, M2, M6+, IDEA.

16. (Currently Amended) The apparatus of claim 10 further comprising:

a combiner;

a decryption module, coupled to said combiner and said storage media device, adapted to receive key information from said combiner and encrypted content and key from said storage media device and to generate clear text content; and

an encryption module, coupled to said decryption module, for encrypting said clear text content with a second negotiated key.

17. (New) The method of claim 1, wherein the bus complies with an IEEE 1394 protocol.

18. (New) A machine-readable medium including instructions executable by a processor for transferring encrypted content via a bus in a system where keys are periodically changed, the machine-readable medium comprising one or more instructions for:

receiving the encrypted content via the bus;

receiving a first key for decrypting the encrypted content;

encrypting the first key with a second key to form an encrypted first key;

combining the encrypted content with the encrypted first key to form a combined encrypted content;

storing the combined encrypted content on a storage media;

in response to a request for the stored encrypted content, decrypting the encrypted content to obtain clear text content;

encrypting the clear text content with a third key; and

transmitting the encrypted content via the bus.